Amendments to the Claims:

Claims 1-6 (Canceled).

Claim 7. (Currently amended): A method for initializing a security token for a mobile device comprising the following steps:

a) transferring a root certificate of a certification authority into said security token using a secure transmission environment,

b) securing the root certificate against modifications , and

c) storing a verification component into said security token allowing use or replacement of a user certificate only when said user certificate is authenticated by said root certificate, and

d) creating a user digital signature in the security token using a private key assigned to the security token, wherein said authentication by said root certificate further comprises

e) verifying a digital signature of the certification authority stored in the security token using a public root key of the certification authority.

Claim 8. (Cancelled).

Claim 9. (Currently amended): A method for ~~authenticating information generated by an application using a security token~~ ~~according to claim 1~~ securely storing a user certificate into a security token contained in a mobile device, wherein the security token comprises a certification authority root certificate, comprising the ~~steps of~~:

a) retrieving a public root key from said root certificate,

b) generating a HASH over a user certificate using ~~the~~ a HASH algorithm specified in said user certificate,

c) retrieving and decrypting a digital signature contained in said user certificate by applying said public root key resulting in a HASH of said user certificate, and

d) ~~allowing use of said user certificate for~~ signing said ~~information~~ user certificate with said digital signature when both HASHs are identical.

Claims 10-11 (Cancelled).

Claim 12. (Original): A method according to claim 9, further comprising the step of:

checking the validity of the root certificate before retrieving said public root key.

Claim 13. (Currently amended): A method for replacing a user certificate stored in a security token ~~according to claim 1~~ in a mobile device, wherein the security token comprises a certification authority root certificate, comprising the steps of:

a) receiving a new user certificate from ~~the~~ a certification authority and storing it into ~~said EEPROM of~~ said security token as a temporary object,

b) generating a HASH over ~~a~~ the new user certificate using a HASH algorithm specified in said new user certificate,

c) retrieving a digital signature contained in said new user certificate and decrypting said digital signature by applying a public root key retrieved from a certification authority root certificate resulting in a HASH of said user certificate, and

d) permanently storing said new user certificate in the security token when both HASHs are identical.

Claims 14-15 (Canceled).

Claim 16. (Currently amended): A Computer program product ~~stored on~~ comprising a computer-readable media containing software instructions for ~~performing of the method according to claims 7 to 13~~
initializing a security token for a mobile device, which instructions when executed by a computer perform the following steps:

a) transferring a root certificate of a certification authority into said security token using a secure transmission environment,

b) securing the root certificate against modifications , and

c) storing a verification component into said security token allowing use or replacement of a user certificate only when said user certificate is authenticated by said root certificate, and

d) creating a user digital signature in the security token using a private key assigned to the security token, wherein said authentication by said root certificate further comprises

e) verifying a digital signature of the certification authority stored in the security token using a public root key of the certification authority.